# Udveksling af metadata mellem SP og IDP

## Før udveksling:

sp.anysoft.dk

Web.config:
SigningCertificate=<ThumbPrint for SP signing certificate>

idp.anysoft.dk:20001

Folder: idp-metadata/idpConfig.xml
Indeholder thumbprint for IDP signing certificate

## Overførsel af idp metadata til sp:

sp.anysoft.dk

Folder: idp-metadata/

**2- Kopieres til**

**Metadata.xml**

**1 - Vælg Link:**
**Download Metadata**

idp.anysoft.dk:20001

## Overførsel af sp metadata til idp:

sp.anysoft.dk

Folder: idp-metadata/

**1 – Call Endpoint:**
**/metadata.ashx**

**Metadata.xml**

**2- Choose file+**
**upload metadata**

idp.anysoft.dk:20001

Folder: idp-metadata/spmetadata/<sp metadata filer>

# ***Brug af encryption / Signerings-nøgler***

sp.anysoft.dk

idp.anysoft.dk:20001

Asymmetriske RSA nøgler (kommer fra configuration)
SP_PRIV_KEY (kommer fra web.config SigningCertificate)
IDP_PUB_KEY (kommer fra idp-metadata fil)

Symmetriske nøgler (Aes) dannes ved behov.

Asymmetriske RSA nøgler (kommer fra configuration)
IDP_PRIV_KEY (kommer fra idpConfig.xml)
SP_PUB_KEY (kommer fra sp-metadata fil)

Symmetriske nøgler (Aes) dannes ved behov.

Kendskab til nedenstående regler gør forståelsen af kilde koden en del lettere:

Signering udføres med en RSA Private key of verificeres med den tilhørende Public key

RSA encryption udføres med en RSA Public key of decrypteres med den tilhørende Private key